# Fall 2014
# SEI Research Review
# Insider Threat Mitigation
# LINE Project

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Andrew P. Moore
Dr. William Claycomb
28-30 October 2014



© 2014 Carnegie Mellon University

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **28 OCT 2014** | **N/A** | |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Insider Threat Mitigation LINE Project** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| **Claycomb /Andrew P. Moore William** | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| **Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213** | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release, distribution unlimited.**

13. SUPPLEMENTARY NOTES
**The original document contains color images.**

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **SAR** | **12** | |

Copyright 2014 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0001753



© 2014 Carnegie Mellon University

# Team

SEI team members

- Dr. Bill Claycomb (Co-PI)
- Andy Moore (Co-PI)
- Dr. Jason Clark
- Matt Collins
- Dr. Jen Cowley
- Bill Novak
- Dr. Bronwyn Woods

Engaged Stakeholders

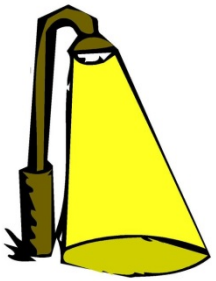
- Two engaged USG partners - data and piloting

Collaborators

- CMU-CS (FY14-15)
  - Prof. Kathleen Carley
  - Neal Altman (staff)
  - Jeff Reminga (staff)
  - Geoff Morgan (student)
  - Matt Benigni (student)
- UC-Davis (FY15)
  - Prof. Sean Peisert
  - Julie B. Ard (student)


© 2014 Carnegie Mellon University

# Project Framing



**Objective:** Develop scientifically and operationally validated insider threat indicators

- **Need:** DoD/Gov't agencies, contractors struggling to build mandated Insider Threat Programs, per Executive Order 13587
- **Challenges:** - Attacks are costly but relatively infrequent
  - Malicious and benign behaviors difficult to distinguish

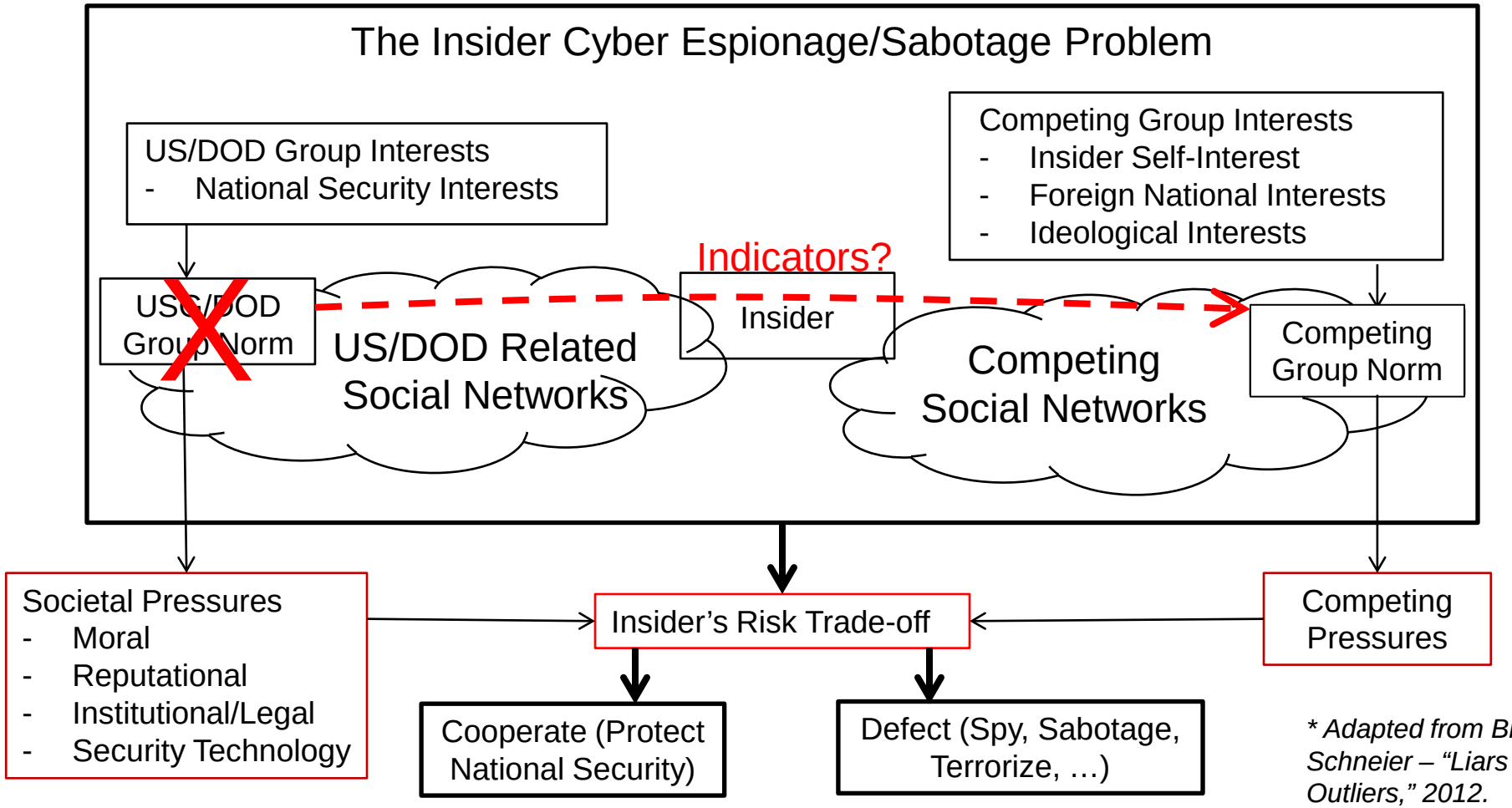
**FY14 Focus:** Dynamic analysis of *social networks* of convicted *spies*

BUT Insiders are not top actors – changes in relationships are key

- **Hypothesis:** Over time, insider social networks exhibit weakening of internal connections, AND the strengthening of external connections to adversaries
- **Data:** ~140 insider espionage incidents – from court records, media reports
- **Data Analysis method:** Measure connection strength over time between insider and family/coworkers/adversaries (ORA toolset)
- **Connection strength measures:** communication frequency, reciprocity, time spent, volume, affect, truthfulness (in order of ease/integrity of measurement)


© 2014 Carnegie Mellon University

# Context for Understanding Insider Behavior *




** Adapted from Bruce Schneier – "Liars and Outliers," 2012.*


© 2014 Carnegie Mellon University

# Preliminary Observations from Incident Data

Broadly specified social networks of ~140 insider spies

- Showed increasing reliance on electronic means of illicit transfer/comms

Elaborated the time series of two incidents

- John Walker (and Walker spy ring)
- Private Bradley Manning (Wikileaks)

Hypothesis supported but situation more complex than framed

- Internal connections may weaken or strengthen over time
- Insider starts connecting more individuals over time (*betweenness* measure)
- Decrease in ratio of internal connections to external connections
- Excluding ring members, networks grow larger but less densely connecting

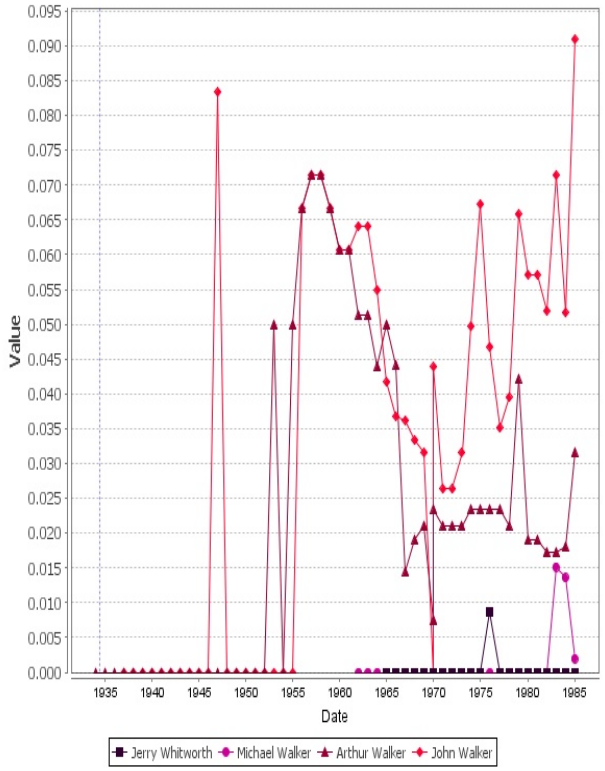
Gain confidence in significance as we compare findings with baseline


© 2014 Carnegie Mellon University

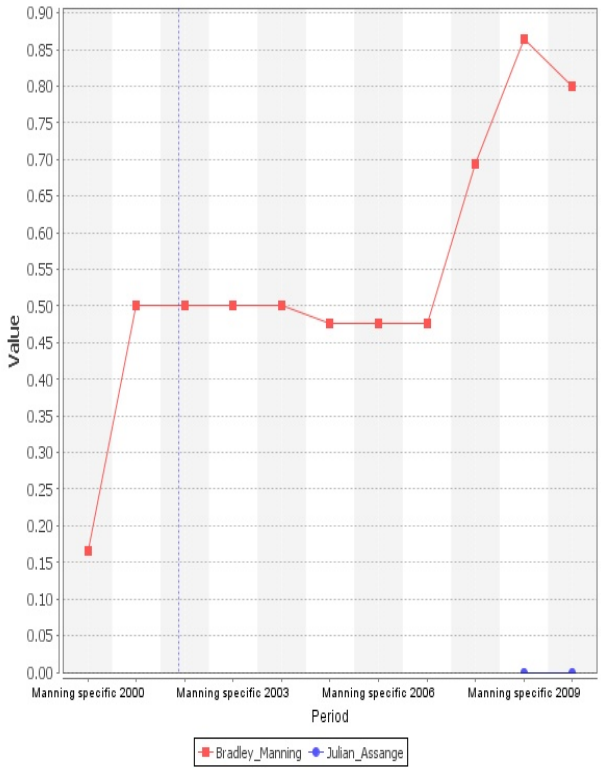
# Increasing betweenness during spy activities – insider starts connecting more individuals

**Come to poster session to see detailed results and talk with analysts!**

## Walker Case



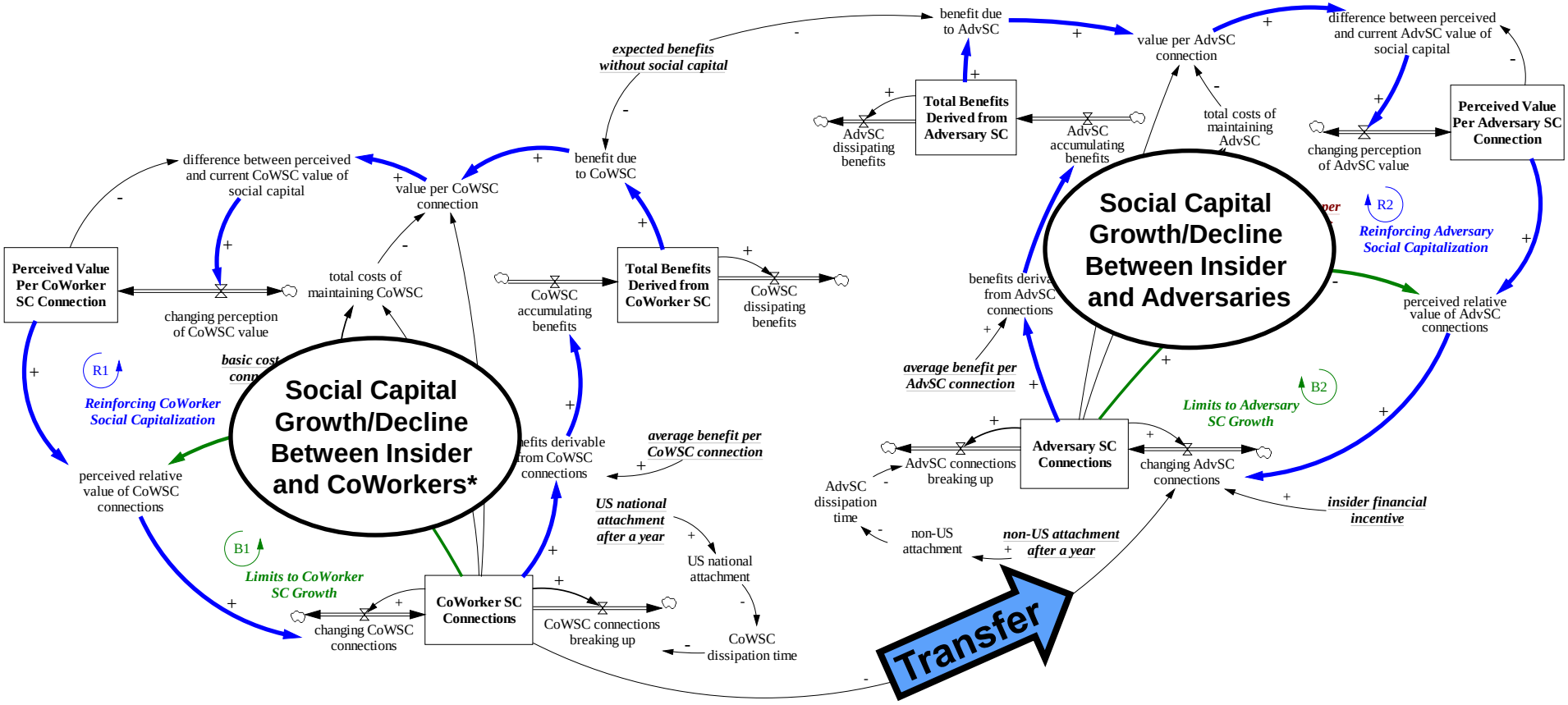

## Manning Case





© 2014 Carnegie Mellon University

# Theory Building: Social Capital Growth/Transfer




* Adapted from Dudley's "The Dynamic Structure of Social Capital: How Interpersonal Connections Create Communitywide Benefits," 22nd Conf. of the System Dynamics Society, 2004.


© 2014 Carnegie Mellon University

# New Work with UC-Davis in FY15

Sociotechnical network (STN) = social network + info flow network

Key Ideas

- Combine analysis of information flow networks with social network analysis
  - earlier detection with lower false positive rates
- Focus not on insider access rights
  - but movement and trajectory of info flow

Compare baseline document flows with actuals (Gemini tool)*

- Identify document (expected) workflows as baseline (up front)
- Compare actual document flows with expected; identify anomalies (real time)
- Requires comparing ***documents to documents*** and ***flows to flows***
- *Proposed Measures*
  - ***Document Similarity*** *:* hashing, plagiarism detection, keyword matching
  - ***Flow Similarity*** *:* graph matching algorithms – eg, using GED measures

* Ard, et.al., “Information Behaving Badly,” NSPW ‘13


© 2014 Carnegie Mellon University

# Plans

## Scientific and Operational Validation

| Method \ Data Set | CERT Incident DB (Open Src) | SEI Emails (Anonymized) | Enron Emails (Public) | Partner Data (Operational) |
|---|---|---|---|---|
| **Insider Social Net Analysis** | FY14 | FY14/15 | FY14/15 | FY15 |
| **Info Flow Net Analysis** | FY15 | FY15 | FY15 | FY15/16 |

## Theory Building

- Ground System Dynamics Model in insider threat risk measures based on sociotechnical net properties

## Transition

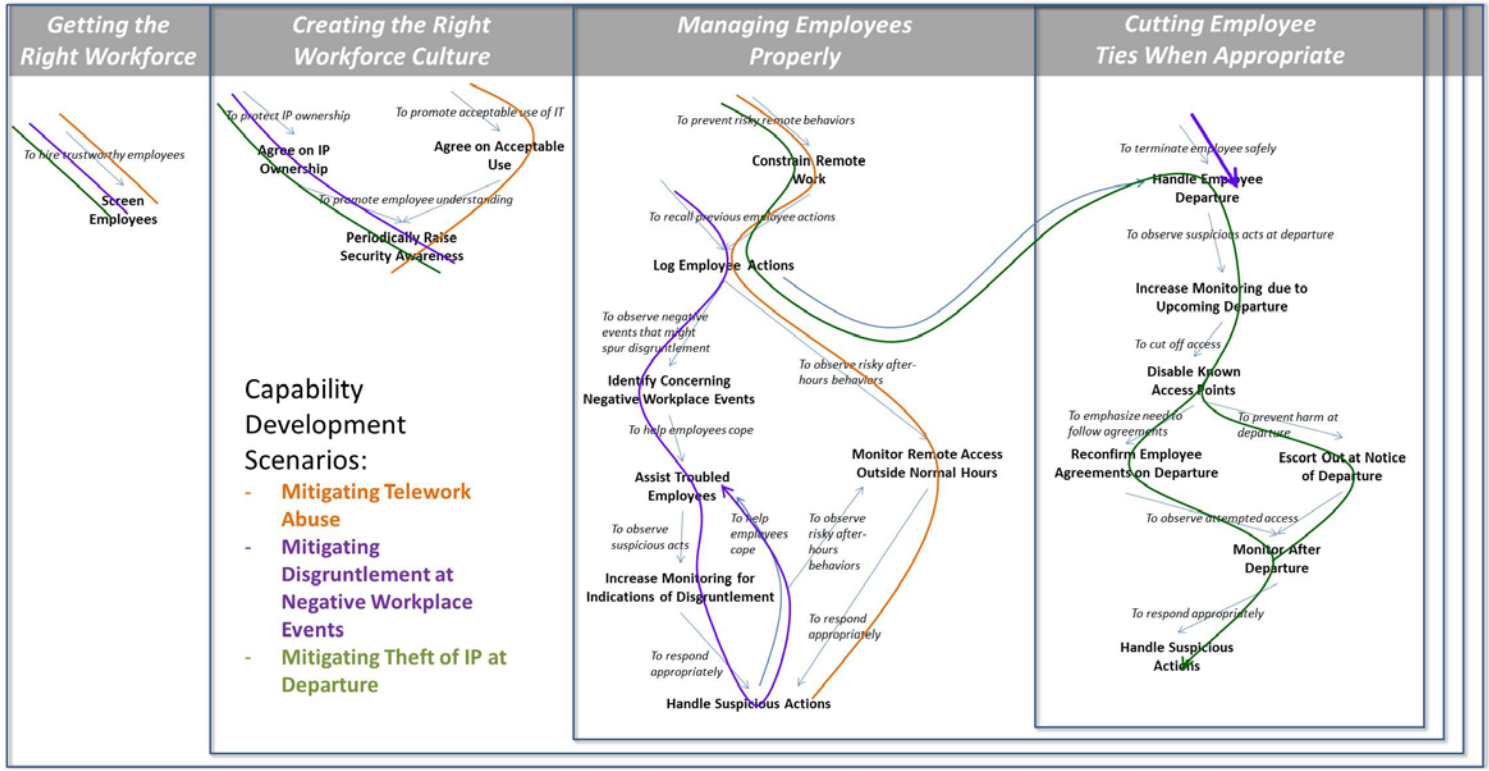
- Developing Special Issue of Journal “Computational and Mathematical Organization Theory” based on Insider Threat ModSim Workshop (7/2014)
- Apply approaches in projects to develop DOD insider threat architectures


© 2014 Carnegie Mellon University

# Publications – Pattern Language as a Transition Vehicle

Research results will continue to ground insider threat mitigation patterns

- 24 patterns identified, 6 analyzed, with 7 ACM/IEEE papers published
- Threat models published in book: *CERT Guide to Insider Threats* (2012)
- *Pattern-Based Design of Insider Threat Programs:* Forthcoming





© 2014 Carnegie Mellon University

# Contact Information Slide Format

**Presenter / Point of Contact**

Andrew P. Moore

CERT Program

Telephone: +1 412-268-5465

Email: apm@cert.org

**U.S. Mail**

Software Engineering Institute

Customer Relations

4500 Fifth Avenue

Pittsburgh, PA 15213-2612

USA

**Web**

www.sei.cmu.edu

www.sei.cmu.edu/contact.cfm

www.cert.org/insider-threat/

**Customer Relations**

Email: info@sei.cmu.edu

Telephone: +1 412-268-5800

SEI Phone: +1 412-268-5800

SEI Fax: +1 412-268-6257



© 2014 Carnegie Mellon University